support. That is, an Internet-based VPN uses the open, distributed infrastructure of the Internet to transmit data between corporate branches.--

Replace the paragraph on page 2, line 21, beginning with "Since each of the" with the following text:

--Since each of the corporate branches is connected to the Internet in the Internet-based VPN, information can be exchanged between the VPN users and the Internet users. This information exchange presents a challenge to protect information located on the corporate branches from unauthorized access by the Internet users and from unauthorized export by the VPN users. For example, hackers have been able to erase files or disks, cancel programs, retrieve sensitive information and even introduce computer viruses, Trojan horses and/or worms into the corporate main branch.--

Replace the paragraph on page 3, line 6, beginning with "A firewall" with the following text:

--A firewall is a technique for keeping a network secure. The firewall is widely used to separate corporate public resources, e.g., DMZ (Demilitarized Zone) servers including a corporate public Web server, mail server, etc., from a corporate internal network as well as to give the VPN users access to the Internet in a secure fashion.--

Replace the paragraph on page 5, line 14, beginning with "In accordance with" with the following text:

--In accordance with one aspect of the present invention, there is provided an integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from the internal network or external network, comprising a packet duplicating module for receiving and duplicating an incoming packet from one of the internal and external networks, a black zone server coupled to the packet duplicating module for analyzing the duplicated packet, and an inspection engine coupled to the packet duplicating module and the black zone server for inspecting whether the received incoming packet corresponds to the selected packet to be blocked based on the analysis in the black zone server, wherein the black zone server serves as at least one of an intrusion detection system, an anti-virus system and a noxious site blocking system.--

Replace the paragraph on page 6, line 26, beginning with "Figs. 3A and 3B" with the following text:

a4

--Figs. 3A and 3B offer schematic diagrams of conventional and other Internet-based VPNs;--

Replace the paragraph on page 12, line 5, beginning with "The first memory" with the following text:

a5

--The first memory 30 is used to store the packet, an OS (operating system), OS parameters, pre-defined parameters, IP addresses, etc. The first memory 30 includes several types of high speed memory devices such as a DIMMM type 64-512 Mybte SDRAM, a flash type 4-8 Mbyte ROM. The first memory 30 further stores instructions for controlling actions to take on the incoming and outgoing packets. These instructions include a predetermined set of criteria based upon the fields of the incoming and other information such as the time of day at which the incoming packet was sent or received, and the state of the session. Such criteria can be implemented by inspecting the fields of the incoming packets, by reference to external data such as a connection status and the time of day and by reference to pre-defined tables or other information stored in the first memory 30. The application of the criteria leads one or several pre-defined actions to be taken on the incoming packet.--

Replace the paragraph on page 12, line 23, beginning with "The VPN processor" with the following text:

--The VPN processor 60 performs tunneling using the IPSec (Internet Protocol Security) protocol, data encryption/decryption and packet authentication. It should be appreciated that the VPN processor 60 and the firewall processor 10 can be implemented by a single micro-processor or by a multiplicity of micro-processors in the present invention.--

In the Claims:

Marked up version of revised claim 1, showing insertions and deletions, is included in Appendix B.

Rewrite claim 1 as follows:

a6

--1. An integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from the internal network or external network, comprising: